Interner Verteilerschlüssel:
(A) [ ] Veröffentlichung im ABl.
(B) [ ] An Vorsitzende und Mitglieder
(C) [ ] An Vorsitzende
(D) [X] Keine Verteilung

Datenblatt zur Entscheidung vom 17. April 2012

Beschwerde-Aktenzeichen: T 0375/09 - 3.5.05

Anmeldenummer: 02450095.1

Veröffentlichungsnummer: 1259046

IPC: H04L 29/06, G06F 1/00, G07F 19/00

Verfahrenssprache: DE

Bezeichnung der Erfindung:
Anlage für die sichere Durchführung von Transaktionen mittels mehrerer Authentifizierungscodes

Patentinhaber:
Losekamm, Arthur Werner Robert

Einsprechende:
ERSTE BANK DER OESTERREICHISCHEN SPARKASSEN AG
s IT SOLUTIONS AT SPARDAT GmbH

Stichwort:
Sicherer Verbindungsaufbau mittels Zusatzcode/ERSTE BANK et al.

Relevante Rechtsnormen:
EPÜ Art. 52(1), 54(2), 56, 83, 100(a)(b)

Schlagwort:
"Ausreichende Offenbarung (ja)"
"Breite Auslegung des Hautpanspruchs (ja)"
"Erfinderische Tätigkeit (ja)"

Zitierte Entscheidungen:
-

Orientierungssatz:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Aktenzeichen: T 0375/09 - 3.5.05

E N T S C H E I D U N G
der Technischen Beschwerdekammer 3.5.05
vom 17. April 2012

Beschwerdeführerin: (gemeinsame Einsprechende)
ERSTE BANK DER OESTERREICHISCHEN SPARKASSEN AG
Graben 21
A-1010 Wien (AT)

s IT SOLUTIONS AT SPARDAT GmbH
Geiselbergstrasse 21-25
1110 Wien (AT)

Vertreter:
Heger, Georg
Sonn & Partner Patentanwälte
Riemergasse 14
A-1010 Wien (AT)

Beschwerdegegner: (Patentinhaber)
Losekamm, Arthur Werner Robert
In der Flaksiedlung 2
A-4060 Leonding (AT)

Vertreter:
Hübscher, Helmut
Patentanwaltskanzlei Hübscher
Postfach 411
A-4010 Linz (AT)

Angefochtene Entscheidung:
Entscheidung der Einspruchsabteilung des Europäischen Patentamts, die am 3. Dezember 2008 zur Post gegeben wurde und mit der der Einspruch gegen das europäische Patent Nr. 1259046 aufgrund des Artikels 101 (2) EPÜ zurückgewiesen worden ist.

Zusammensetzung der Kammer:

Vorsitzende: A. Ritzka
Mitglieder: M. Höhn
F. Blumer

Sachverhalt und Anträge

I. Die Beschwerde richtet sich gegen die Entscheidung der Einspruchsabteilung, zur Post gegeben am 3. Dezember 2008, mit der der Einspruch gegen das Europäische Patent mit der Nr. 1259046 zurückgewiesen wurde. Der Einspruch ist im wesentlichen gestützt auf Einwände unter Artikel 100 (a) mit Artikel 52(1), 54 und 56 EPÜ sowie Artikel 100 (b) mit Artikel 83 EPÜ.

In der vorliegenden Entscheidung wird verwiesen auf (die Nummerierung folgt den Bezeichnungen im Einspruchs- und Beschwerdeverfahren):

E10: Raimund Christoph Fitz: Der Zahlungsverkehr mittels Telebanking und Chipkarte unter besonderer Berücksichtigung von Sicherheitsaspekten (Diplomarbeit der Sozial- und Wirtschaftswissenschaftlichen Fakultät der Universität Wien, September 1996, Seiten 160-163 und 213-219),

E11: Timo Bereuter: Electronic Banking (Diplomarbeit der Sozial- und Wirtschaftswissenschaftlichen Fakultät der Universität Wien, März 1996, Seiten 50-54),

E12: Memo Nr. 2965 der Network Working Group betreffend HTTP State Management Mechanism vom Oktober 2000,

E13: Memo Nr. 2109 der Network Working Group betreffend HTTP State Management Mechanism vom Februar 1997,

E14: EP 1065634 A1,

E15: WO 01/17310 A1,

E16: EP 0844551 A2,

E17: Gegenüberstellung in Auslegung des Patentanspruches des von der Beschwerdeführerin verwendeten Netbanking-Verfahrens und des korrespondierenden Österreichischen Stammpatents AT 411 947 B zum gegenständlichen Streitpatent, vorgelegt mit Schreiben vom 22.09.2005 an die ERSTE BANK und

E18: DE 19718103 A1.

II. Die Beschwerdeschrift wurde am 3. Februar 2009 eingereicht. Die Beschwerdegebühr wurde am selben Tag entrichtet. Die Beschwerdeführerin (gemeinsame Einsprechende) beantragte in der am 3. April 2009 eingereichten Beschwerdebegründung, die angefochtene Entscheidung der Einspruchsabteilung aufzuheben und das Patent in vollem Umfang zu widerrufen sowie hilfsweise eine mündliche Verhandlung anzuberaumen.

III. Der Beschwerdegegner (Patentinhaber) beantragte in seiner Erwiderung vom 26. August 2009, die Beschwerde zurückzuweisen und das Streitpatent in vollem Umfang aufrecht zu erhalten, hilfsweise eine mündliche Verhandlung anzuberaumen.

IV. Mit einem Bescheid vom 14. Dezember 2011 wurden die Parteien zur mündlichen Verhandlung am 17. April 2012 geladen. In einem Anhang zur Ladung zur mündlichen Verhandlung brachte die Kammer ihre vorläufige Meinung zum Ausdruck, dass der Gegenstand des Streitpatents ausreichend offenbart sei (Artikel 100b mit 83 EPÜ), aber auch entsprechend breit ausgelegt werden müsse. Die Beschwerdeführerin habe jedoch auch bei breiter Auslegung in der Beschwerdebegründung noch nicht überzeugend dargelegt, dass der Gegenstand von

Anspruch 1 nahegelegt sei (Artikel 100a mit 56 EPÜ). Die Kammer legte in dem Anhang auch ihre Gründe für diese vorläufige Auffassung dar.

Die Argumentation der Beschwerdeführerin zur Neuheit sei zu pauschal und enthalte eher Argumente gegen die erfinderische Tätigkeit. Vor allem fehle bisher ein druckschriftlicher Beleg des Fachwissens bezüglich der von der Beschwerdeführerin angeführten "Browsertechnologie". Die Kammer vertrat die vorläufige Auffassung, dass eine breite Interpretation von Anspruch 1 im Sinne der E17 möglich ist. Insbesondere schienen der Kammer die Argumente der Beschwerdeführerin bezüglich der "Browsertechnologie" und den dabei verwendeten "Session-Keys" bzw. der Verwendung von "Hash-Codes" am bedeutsamsten und damit ein Schwerpunkt für die Diskussion in der mündlichen Verhandlung zu sein. Obwohl die Dokumente E10 und E11 diesbezüglich relevant zu sein schienen, sei der Kammer keine abschließende Beurteilung möglich, da bisher von beiden Seiten nur pauschale Argumente vorgetragen worden seien. Im Rahmen der mündlichen Verhandlung sei daher zu klären, ob der Gegenstand von Anspruch 1 bei einer breiten Interpretation ausgehend von E14 oder E18 kombiniert mit dem allgemeinen Fachwissen bezüglich der "Browsertechnologie" und den dabei verwendeten "Session-Keys" bzw. der Verwendung von "Hash-Codes" nahegelegt sei. Jedoch habe die Beschwerdeführerin dieses Fachwissen bisher nicht ausreichend belegt.

V. Mit Schreiben vom 15. März 2012 übermittelte die Beschwerdeführerin (gemeinsame Einsprechende) als Beleg für dieses Fachwissen folgende Dokumente zusammen mit weiteren Argumenten dazu, weshalb der Gegenstand von

Anspruch 1 des Streitpatents nicht neu sei oder zumindest nicht auf einer erfinderischen Tätigkeit beruhe:

E19: Secure Hash Standard (17. April 1995),
E20: Menezes, van Oorschot, Vanstone "Handbook of Applied Cryptography", Kapitel 9, CRC Press, 1996,
E21: EP 0 695 985 A1.

VI. Am 17. April 2012 fand eine mündliche Verhandlung statt, in deren Verlauf alle Einwände der Beschwerdeführerin erörtert wurden. Die Beschwerdeführerin reichte während der Verhandlung einen Auszug aus Wikipedia betreffend "Transport Layer Security" einschließlich Skizze (siehe Anlage zum Protokoll der mündlichen Verhandlung) ein. Die Beschwerdegegnerin beantragte dieses spät in das Verfahren eingebrachte Dokument nicht zuzulassen.

VII. Der unabhängige Anspruch 1 gemäß dem Hauptantrag (d.h. des erteilten Patents) lautet:

"Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal (102), das zur Eingabe einer Benutzerkennung dient, mit einer Auswerteeinheit (106), die mit dem Terminal (102) über ein primäres Netz (101) verbunden ist, und im wesentlichen aus einer Speicher- und Prozessoreinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, mit einem Codegenerator, der einen Sicherheitscode erzeugt, mit einer Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108) sendet, und mit einer Eingabemöglichkeit für den Sicherheitscode am Terminal

und einer Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit (106), dadurch gekennzeichnet, daß die Auswerteeinheit (106) einen zusätzlichen Codegenerator zur Erstellung eine Zusatzcodes aufweist und eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes aufweist, wobei das Terminal neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist und die Auswerteeinheit (106) derart ausgestaltet ist, daß diese den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert."

VIII. Die Beschwerdeführerin (gemeinsame Einsprechende) beantragte die Aufhebung der angefochtenen Entscheidung und den Widerruf des europäischen Patents Nr. 1259046.

Der Beschwerdegegner (Patentinhaber) beantragte die Zurückweisung der Beschwerde.

IX. Am Ende der mündlichen Verhandlung verkündete die Kammer ihre Entscheidung.

Entscheidungsgründe

1.1 Zulässigkeit der Beschwerde

Die Beschwerdeschrift und die Beschwerdebegründung wurden wirksam und fristgerecht eingereicht. Die

Beschwerdegebühr wurde ebenfalls fristgerecht entrichtet. Die Beschwerde ist daher zulässig.

1.2 Zulassung des in der Verhandlung vorgelegten Dokuments in das Verfahren

Da die Beschwerdeführerin weder die genaue Herkunft, noch das Veröffentlichungsdatum des in der Verhandlung vorgelegten Dokumentes (siehe Sachverhalt VI.) belegen konnte, konnte die Kammer dieses Dokument nicht im Verfahren berücksichtigen.

2. Offenbarung (Artikel 100(b) mit 83 EPÜ)

2.1 Die Beschwerdeführerin argumentierte zum Einspruchsgrund nach Artikel 100b EPÜ, dass eine ausreichende Offenbarung fraglich sei, wenn man die sehr breite Auslegung der Begriffe "Eingabe" (im Sinne einer Brockhaus-Definition als Übertragen von Daten aus einem peripheren Gerät in den Arbeitsspeicher eines Computers) und "Ausgabe" (im Sinne einer Brockhaus-Definition als Übertragen von Daten oder Programmen eines Computers an ein externes Ausgabegerät) in Anspruch 1 zugrunde lege, so wie in E17 vom Patentinhaber selbst vorgenommen. In E17 werde dezidiert festgestellt, dass eine Ausgabe des Zusatzcodes nicht zwingend optisch für den Benutzer sichtbar erfolgen müsse und eine Eingabe auch nicht zwingend manuell vom Benutzer vorgenommen werden müsse. Vielmehr sei auch eine automatische Eingabe/Ausgabe im Sinne der obigen Brockhaus-Definitionen umfasst. Die Beschwerdeführerin verwies diesbezüglich auf "Hash Codes" und "Session keys" als Zusatzcodes. Dafür gebe es aber im Streitpatent keine ausreichende Offenbarung. Im Sinne einer ausreichenden Rechtssicherheit sei daher

entweder der Patentanspruch im Rahmen der Offenbarung eng auszulegen, oder aber die Erfindung sei nicht über die ganze Breite des Anspruchs ausreichend offenbart.

2.2 Der Beschwerdegegner (Patentinhaber) argumentierte im wesentlichen, dass die E17 lediglich eine auf einer "privaten Meinung" beruhende Auslegung darstelle und die Frage einer unzulässig breiten Auslegung des Hauptanspruchs nicht Sache der Beschwerdekammer sein könne. Im übrigen sei für den Fachmann aufgrund seines Fachwissens offensichtlich, wie eine Eingabe- und Ausgabemöglichkeit für einen Zusatzcode aussehen könne.

2.3 Die Kammer interpretiert die Argumentation des Beschwerdegegners dahingehend, dass der Fachmann die nötigen Schritte zwischen den Zeilen mitliest, auch wenn nur für die sichtbare bzw. optische Eingabe/Ausgabe explizit eine Offenbarung in der Patentschrift besteht (vgl. Abschnitte [0006] und [0007], Figur 2, Schritte 211 bis 213 und 215).
Der Einwand der Beschwerdeführerin ist auch auf eine mangelnde Stützung des breiten Anspruchs 1 durch die Beschreibung gerichtet. Jedoch ist Artikel 84 EPÜ kein Einspruchsgrund und daher auch nicht Gegenstand dieses Beschwerdeverfahrens. Somit stellt sich der Einwand der Beschwerdeführerin für die Kammer so dar, dass der Anspruch 1 nicht im gesamten beanspruchten Bereich offenbart sei (Artikel 83 EPÜ).

Nach Auffassung der Kammer ist diese Problematik jedoch weniger eine Frage der Offenbarung, denn die Kammer teilt die Auffassung der Beschwerdegegnerin, dass Eingabe- und Ausgabemöglichkeiten für einen Zusatzcode fachnotorisch bekannt waren.

3. Mangelnde Neuheit oder erfinderische Tätigkeit (Artikel 100(a) mit 52(1), 54(2) und 56 EPÜ)

Die breite Auslegung des Hauptanspruchs im Sinne der Interpretation nach E17 (siehe Punkt 2.1) ist auch bei der Interpretation des angezogenen Standes der Technik zugrunde zu legen.

3.1 Die Einspruchsabteilung argumentierte, dass zumindest das Merkmal, wonach ein Zusatzcode über das primäre Netz von der Auswerteeinheit zum Terminal geschickt wird, und dass auch der Zusatzcode zur Autorisierung einer Transaktion verwendet wird, aus keinem der angezogenen Dokumente eindeutig und zweifelsfrei offenbart sei. Der Hauptanspruch sei daher neu.

3.2 Hiergegen wandte sich die Beschwerdeführerin mit der Beschwerde im wesentlichen mit dem Argument, dass vor dem Hintergrund der möglichen breiten Auslegung der Begriffe "Eingabe" und "Ausgabe" (siehe Punkt 2.1 oben bzgl. E17) sämtliche Merkmale des Anspruchs 1 zumindest implizit offenbart seien. Neben der E14 als nächstliegendem Stand der Technik offenbare auch die E18 eine TAN als Sicherheitscode i.S.d. Anspruchs 1 neben dem "selbstverständlich auch andere Codes oder Daten, die dem Zusatzcode gemäß dem Streitpatent entsprechen" übertragen werden könnten. Die Beschwerdeführerin verwies diesbezüglich pauschal auf in der Browsertechnologie übliche Codes, welche die Einzigartigkeit einer Benutzersitzung zwischen dem Autorisierungsrechner und dem Dateneingabegerät gewährleisten. Als Beispiel führte die Beschwerdeführerin den in der E17 dargestellten Session-

Key bzw. sh-Code an. Ein solcher Zusatzcode sei implizit auch aus der E14 oder der E18 bekannt. Zusätzlich sei in E18 auch ein Passwort offenbart, welches auch als Zusatzcode gemäß Anspruch 1 des Streitpatents angesehen werden könne.

Weiter wurde ebenfalls pauschal auf eine mögliche zusätzliche Verschlüsselung der Daten zur weiteren Erhöhung der Sicherheit verwiesen, wozu bestimmte Schlüssel erforderlich seien, die Zusatzcodes darstellten, welche zwischen Auswerteeinheit und Terminal übertragen würden.

Zumindest fehle die erfinderische Tätigkeit, denn auch sog. Hash-Codes fielen unter den Schutzbereich von Anspruch 1 und wären bei einer breiten Auslegung als Zusatzcodes anzusehen. Die Beschwerdeführerin verwies diesbezüglich pauschal auf die Druckschriften E10 bis E13, E15 und E16.

3.3 Der Beschwerdegegner entgegnete im wesentlichen, dass weder die E14, noch die E18 über die Merkmale des Oberbegriffs hinausgehe. Die bloße Möglichkeit, zusätzliche Codes vorzusehen, sei vage und mache die Offenbarung der E14 oder E18 keinesfalls neuheitsschädlich. So offenbare die E18 nicht einmal einen zusätzlichen Codegenerator. Das von der Beschwerdeführerin in der E18 erwähnte Passwort entspreche der Benutzerkennung im Oberbegriff von Anspruch 1, da es bereits vor dem Verbindungsaufbau eingegeben werde, und entspreche damit nicht einem Zusatzcode, welcher erst nach dem Verbindungsaufbau eingegeben werde. Anspruch 1 sei daher neu gegenüber der E14 oder der E18.

Im übrigen sei von Bedeutung, dass der Zusatzcode gemäß Anspruch 1 individuell für den Autorisierungsvorgang erstellt werde und über das primäre Netz an das Terminal geschickt werde, von wo dieser Zusatzcode gemeinsam mit dem Sicherheitscode wieder an die Auswerteeinheit zurück gesendet werde.

Hash-Codes dienten "zur Absicherung einer korrekten Datenübertragung, nicht aber zur Überprüfung, ob die Daten von einem autorisierten Benützer übertragen wurden". Daher habe ein Fachmann keinen Anlass, bekannte Maßnahmen wie z.B. Hash-Codes bei der Absicherung eines Zugangs zur Durchführung von Transaktionen heranzuziehen. Der Gegenstand von Anspruch 1 werde dadurch somit nicht nahegelegt.

Die E15 lege den Gegenstand von Anspruch 1 auch nicht nahe, weil der übermittelte Token über das sekundäre Netz an die Auswerteeinheit zurück übertragen werde. Bei der E16 hingegen fehle jeder Hinweis auf einen Zusatzcode. Der Gegenstand von Anspruch 1 sei damit ausgehend von keinem der genannten Dokumente nahegelegt.

4. Der Beschwerdegegner hatte keine Einwände gegen die Zulassung der mit der Beschwerdebegründung vorgelegten Dokumente E17 und E18 sowie auch nicht gegen die verspätet nach der Anberaumung der mündlichen Verhandlung vorgelegten E19 bis E21. Die Kammer hat diese Dokumente ins Verfahren zugelassen, insbesondere da E19 bis E21 in Reaktion auf die im Ladungsbescheid aufgeworfenen Fragen vorgelegt wurden.

5. Die Argumentation der Einspruchabteilung erscheint der Kammer insgesamt überzeugend. Jedoch liegt dieser Argumentation nicht die oben erwähnte gebotene breitere Interpretation von "Eingabe" und "Ausgabe" zu Grunde. In der mündlichen Verhandlung wurde daher vor allem diskutiert, ob und inwieweit sich durch diese Interpretation ein anderes Ergebnis ergibt, insbesondere wenn man eine elektronische Übermittlung und Eingabe des Zusatzcodes mit unter den Anspruchswortlaut liest.

5.1 Es war im Verfahren von allen Seiten unbestritten, dass E14 alle Merkmale des Oberbegriffs von Anspruch 1 offenbart (vgl. z.B. Zusammenfassung mit den Figuren 2a und 2b). Ebenso war es unbestritten, dass E18 diese Merkmale von Anspruch 1 offenbart (vgl. z.B. Spalte 1, Zeile 39 bis Spalte 2, Zeile 25). Beide Dokumente sieht die Kammer als einschlägig und damit geeignet als Ausgangspunkt zur Beurteilung von Neuheit und erfinderischer Tätigkeit an.

5.2 Das im Einspruchsverfahren (siehe Schreiben vom 01. Oktober 2008, Seite 3) vorgetragene Argument der Beschwerdeführerin mit Hinweis auf Abschnitt [0054] von E14, der einen zusätzlichen "User access code" oder ein Passwort vorsieht, die dem Zusatzcode gemäß dem kennzeichnenden Teil von Anspruch 1 entsprächen, überzeugt die Kammer nicht. Vielmehr teilt die Kammer die Auffassung des Beschwerdegegners, dass das erwähnte Passwort der Benutzerkennung im Oberbegriff von Anspruch 1 entspricht, da es bereits vor dem Verbindungsaufbau ("to establish communication") und nicht erst nach dem Verbindungsaufbau eingegeben wird sowie nicht für jede Transaktion generiert wird.

Die E18 entspricht vom Offenbarungsgehalt im wesentlichen der E14. In E18 werden neben der Rückübermittlung einer TAN über einen primären Kanal zwar auch die sogenannten Call-Back-Systeme angesprochen, in denen ein Rückruf über den gleichen Kanal wie die Verbindungsaufnahme, d.h. den primären Kanal, erfolgt. Jedoch wird dies nur als nachteiligere Variante angeführt, der gegenüber die Lehre der E18 als vorteilhaft dargestellt wird. Es mangelt somit an einer Offenbarung der Kombination beider Varianten. Dabei handelt es sich auch nicht um eine der als "Sicherheitsstufen" bezeichneten Varianten (so offenbart ab Spalte 2, Zeile 50), unter denen explizit Kombinationen angeregt sind (siehe Spalte 3, Zeilen 39 und 40). Mit den in E18 (Spalte 3, Zeilen 29 bis 35) erwähnten Passwörtern verhält es sich genauso wie oben anhand der E14 erläutert. Es wird bereits vor dem Verbindungsaufbau und nicht erst danach eingegeben und nicht für jede Transaktion generiert.

Zwar führt auch die E18 allgemein die Verwendung von Verschlüsselung an. Hierbei bleibt aber wiederum offen, wo der/die Schlüssel erzeugt werden und wie genau der Austausch und die Überprüfung erfolgt. Auch liegt der Schwerpunkt auf dem sekundären Kanal (GSM, Pager etc.).

5.3 Weder E14 noch E18 offenbaren somit einen Zusatzcode gemäß den Merkmalen des kennzeichnenden Teils von Anspruch 1. Der Gegenstand von Anspruch 1 ist daher neu im Hinblick auf E14 und E18.

6. Die Beschwerdeführerin hat darüber hinaus argumentiert, dass das Kennzeichen von Anspruch 1 durch das allgemeine Fachwissen nahegelegt sei, insbesondere durch allgemein

bekannte "Hash-codes", "Session-keys" mit SSL-Protokoll sowie durch die bekannte Verwendung von sogenannten "Cookies". Diese könnten jeweils als Zusatzcodes im Sinne von Anspruch 1 interpretiert werden, insbesondere vor dem Hintergrund einer gebotenen breiten Auslegung, weil an den Begriff "Zusatzcode" keine Bedingungen geknüpft seien.

6.1 Die Kammer stimmt zu, dass das Kennzeichen von Anspruch 1 den Begriff "Zusatzcode" nicht näher spezifiziert, weshalb jegliche Information, die in der Auswerteeinheit erzeugt wird, über den primären Kanal an das Terminal gesendet und von dort wieder über diesen Kanal zurück übertragen wird, als Zusatzcode angesehen werden kann.

Die Kammer stimmt dem Argument der Einspruchsabteilung nicht zu, wonach der Zusatzcode explizit zur Autorisierung der Transaktion geprüft werden muss (vgl. z.B. die Seite 6, Absatz 5 i.H.a. Hash-Codes). Anspruch 1 definiert lediglich irgendeine Art von Zusatzcode, der auf Seiten der Auswerteeinheit generiert wird, über den primären Kanal an das Terminal gesendet und nach dem Zurückschicken von der Auswerteeinheit überprüft wird. Es ist somit lediglich erforderlich, dass es nicht zu einer Autorisierung der Transaktion kommt, wenn die Prüfung des Zusatzcodes negativ ausfällt. Es genügt somit nach Anspruch 1, wenn ein Zusatzcode im Rahmen des Datenverkehrs z.B. zu Verschlüsselungszwecken oder zu Zwecken der Gewährleitung von Integrität der Daten überprüft wird. Sollten hierbei Probleme auftreten, so wird in der Regel schon dadurch die Transaktion nicht freigegeben, d.h. autorisiert.

Die dem Kennzeichen zu Grunde liegende Aufgabe wird (in Übereinstimmung mit der Beschwerdeführerin) in der weiteren Erhöhung der Sicherheit einer Transaktion gesehen.

Hash-Codes

6.2 Die Beschwerdeführerin argumentierte bezüglich Hash-Codes, dass E10 (mit Verweis auf Abschnitt 7.3.1.3), E11 (mit Verweis auf Abschnitt 7.2), E19 (mit Verweis auf Seite 2 "Applications" und Figur 1) oder E20 (mit Verweis auf Seite 322, Abschnitt 9.1; Seite 362, Abschnitt 9.78) die Verwendung von Hash-Codes offenbarten, welche als Zusatzcodes i.S.d. Anspruchs 1 anzusehen seien, da Hash-Codes in beiden Richtungen übermittelt und überprüft würden (vgl. z.B. die Eingabe vom 15. März 2012, Seite 2, ab viertem Absatz). Bereits im Einspruchsverfahren (siehe die Eingabe vom 1. Oktober 2008, der die Seiten 2 und 3 verbindende Absatz) argumentierte die jetzige Beschwerdeführerin, dass Hash-Codes bei Web-basierten Transaktionen generiert und übertragen würden. Ein Hash-Code würde z.B. durch einen Web-Server aufgrund einer Prüfsumme erstellt und an das Terminal des Benutzers übermittelt und wieder vom Terminal an den Web-Server zurückgeschickt. Daher handele es sich um einen Zusatzcode nach Anspruch 1.

6.3 Der Beschwerdegegner argumentierte unter anderem, dass Hash-Codes zur Absicherung einer korrekten Datenübertragung dienten, nicht aber zum Aufbau einer sicheren Verbindung oder zur Überprüfung, ob Daten von einem autorisierten Benutzer übertragen wurden (vgl. z.B. Seite 5, zweiter Absatz der Eingabe vom 26. August 2009). Wesentlicher Unterschied gegenüber dem Kennzeichen von

Anspruch 1 jedoch sei, dass Hash-Codes vom Sender zum Empfänger geschickt würden, aber nicht zurück.

6.4 Die Kammer stimmt dem Beschwerdegegner zu, dass Hash-Codes in erster Linie der Gewährleistung von Datenintegrität dienen, d.h. dass die Daten nicht manipuliert werden. Damit geht implizit einher, dass die Daten unverändert vom Benutzer des Terminals kommen.

Die Beschwerdeführerin konnte nicht belegen, dass eine Hash-Funktion tatsächlich fachüblich so verwendet wird wie von ihr argumentiert. Insbesondere konnte die Beschwerdeführerin nicht überzeugend darlegen, dass bei einer Client-Server-Anwendung ein Hash-Code auf der Server-Seite generiert und vom Client zurückkommend wieder empfangen wird.

Die bloße Möglichkeit ist für ein Naheliegen nicht ausreichend, vor allem vor dem Hintergrund der Funktion eines Hash-Wertes. Ein Hash-Code wird anhand der zu übertragenden Nachricht mittels einer bestimmten Funktion ermittelt und mit dem privaten Schlüssel des Senders verschlüsselt übertragen. Auf der Empfängerseite wird der Hash-Code mit dem öffentlichen Schlüssel des Senders entschlüsselt und mittels derselben Funktion aus der empfangenen Nachricht der Hash-Code empfängerseitig erneut ermittelt. Stimmen die beiden Werte überein, so kann der Empfänger davon ausgehen, die Nachricht des Senders unverfälscht erhalten zu haben.

Die Beschwerdeführerin konnte nicht überzeugend darlegen, weshalb dieser Hash-Code nun wieder zum Sender zurück übertragen werden sollte. Dazu besteht vor dem Hintergrund der Aufgabe eines Hash-Codes zur Sicherung

der Datenintegrität auch keine Motivation. Die E10 deutet lediglich den Verwendungsbereich einer Hash-Funktion an, ohne auf die technische Realisierung einzugehen (siehe Abschnitt 7.3.1.3). Die E11 offenbart nur allgemeines Hintergrundwissen über Kryptografie und digitale Signaturen, ohne Hash-Codes explizit anzusprechen. Auch die bezüglich E19 und E20 angeführten Passagen offenbaren nicht zweifelsfrei, dass eine Rückübertragung eines Hash-Codes erfolgt. Dies gilt auch für die in E20 (vgl. Seite 325, Abschnitt 9.7) erwähnten Message Authentication Codes (MAC).

Die Beschwerdeführerin konnte nicht schlüssig darlegen und die Kammer daher nicht überzeugen, dass das Kennzeichen von Anspruch 1 aus dem allgemeinen Fachwissen über Hash-Codes nahegelegt ist.

Session-Keys mit SSL Protokoll

6.5 Was die von der Beschwerdeführerin geltend gemachte "Browsertechnologie" und den dabei verwendeten "Session-Key" betrifft, so stimmt die Kammer dem Beschwerdegegner zu, dass es sich bei einem Session-Key um einen Verschlüsselungscode handelt, der übermittelt wird, um verschlüsseln zu können. Im Rahmen einer SSL-Verschlüsselung (vgl. Abschnitt [0055] der E14) erfolgt ein Austausch des von der Beschwerdeführerin angeführten Session-Keys. Selbst wenn man den Session-Key als Zusatzcode ansieht, der über den primären Kanal ausgetauscht wird, so bleibt fraglich, ob der Session-Key von einem Codegenerator der Auswerteeinheit erzeugt wird. Wesentlicher jedoch ist aus Sicht der Kammer das weitere Argument des Beschwerdegegners, dass dieser Schlüssel nicht hin- und hergeschickt wird. Die

Beschwerdeführerin konnte dies mit keinem der im Verfahren angezogenen Dokumente zum Stand der Technik oder zum Beleg des allgemeinen Fachwissens nachweisen.

6.6 Die Beschwerdeführerin hat zur Stützung ihrer Argumentation bzgl. Session-Keys insbesondere die E21 eingeführt und argumentiert, dass das darin beschriebene Anmeldezertifikat einen Session-Key beinhalte. Das Anmeldezertifikat werde von einer Maschine an einen angemeldeten Benutzer geliefert und von diesem an das verteilte System, also zurück (mit Hinweis auf die Schritte 130 und 136 in Figur 3 mit zugehörigem Text ab Spalte 5, Zeile 37). Die Kammer stimmt jedoch dem Beschwerdegegner zu, der korrekt argumentierte, dass das Anmeldezertifikat mit dem Session-key nicht vom Server des verteilten Systems (distributed system) generiert und geschickt werde, sondern von einer zusätzlichen dritten Einheit. Damit würde der Session-Key nicht hin- und zurückgeschickt. Darüber hinaus habe der Fachmann keine Veranlassung, ausgehend von E14 oder E18 eine zusätzliche dritte Einheit vorzusehen, und würde eine Kombination mit E21 schon deshalb nicht in Betracht ziehen.

6.7 Die Beschwerdeführerin verwies darüber hinaus noch auf die in E21 im Zusammenhang mit Kerberos beschriebenen "tickets" (vgl. ab Spalte 6, Zeile 39 und Figur 4b). Der Beschwerdegegner hielt dem jedoch zu Recht entgegen, dass selbst wenn man solche "tickets" als Zusatzcode im Sinne des Kennzeichens von Anspruch 1 ansehen würde, das Ticket von einer von Client und Server getrennten dritten Einheit, nämlich dem key-distribution-center KDC 109, an den Client gesendet würde (siehe Schritt 174 in Figur 4b). Die Beschwerdeführerin gehe jedoch fehl in

der Annahme, dass das gleiche Ticket an das KDC zurückgesendet werde (so behauptet mit Hinweis auf Schritt 180 in Figur 4b). Vielmehr würde das in Schritt 174 erhaltene Ticket vom Client an den Server AS übertragen. Schritt 180 enthalte andere Informationen, die nicht mehr mit dem Ticket identisch seien. Damit fehle es wiederum daran, dass ein Zusatzcode hin- und zurückgesendet werde. Die Kammer schließt sich dieser Interpretation von E21 an.

Das weitere Argument der Beschwerdeführerin, dass das KDC ja auf dem Server der Bank laufen könnte, ist spekulativ und überzeugt die Kammer nicht, dass der Fachmann eine Kombination von E14 bzw. E18 mit E21 in Betracht ziehen würde.

6.8 Die Beschwerdeführerin konnte somit nicht schlüssig darlegen und die Kammer daher nicht überzeugen, dass das Kennzeichen von Anspruch 1 aus dem allgemeinen Fachwissen über Session-Keys oder aus der Offenbarung von E21 nahegelegt ist.

Cookies

6.9 Die Beschwerdeführerin hat weiter argumentiert, dass sogenannte "Cookies" als Zusatzcodes im Sinne des Kennzeichens von Anspruch 1 angesehen werden könnten und dabei auf E12 und E13 (z.B. Abschnitt 5.1) verwiesen. Die Kammer stimmt jedoch dem Beschwerdegegner zu, dass ein Cookie selbst keinen Code darstellt, sondern nur ein Vehikel zur Aufnahme von Information, z.B. für einen Warenkorb im Rahmen eines Online getätigten Einkaufsvorgangs. Wie aus der zitierten Passage von E13 hervorgeht, wird ein Cookie vom Server generiert und auf

dem Client bzw. User Agent gespeichert. Jedes Mal wenn der Client einen Gegenstand auswählt und in seinen Warenkorb legt, wird dies vom Server in dem clientseitigen Cookie gespeichert. Ein Cookie dient aber nicht dem Verbindungsaufbau und der Verbindungssicherheit. Die Beschwerdeführerin konnte auch nicht überzeugend darlegen, welche der in Abschnitt 5.1 von E13 gezeigten Informationen die Aufgabe eines Zusatzcodes übernehmen könnte.

6.10 Ebenfalls hat der Beschwerdegegner überzeugend argumentiert, dass der Fachmann ausgehend von E14 oder E18 keine Veranlassung gehabt hätte, gerade bei Cookies eine Lösung der objektiven Aufgabe zu suchen, weil Cookies allgemein als besonders sicherheitskritisch einzustufen seien und gerade nicht der Erhöhung der Sicherheit dienten, sondern zusätzliche Risiken schafften.

6.11 Die Beschwerdeführerin konnte somit nicht schlüssig darlegen und die Kammer daher nicht überzeugen, dass das Kennzeichen von Anspruch 1 aus dem allgemeinen Fachwissen über Cookies nahegelegt ist.

6.12 Die Kammer stimmt dem Beschwerdegegner weiter zu, dass E15 den Gegenstand von Anspruch 1 auch nicht nahelegt, weil der übermittelte Token über das sekundäre Netz an die Auswerteeinheit zurück übertragen wird. Bei der E16 konnte die Beschwerdeführerin nicht darlegen, welcher Teil der Offenbarung einen Zusatzcode gemäß dem Kennzeichen von Anspruch 1 nahelegen soll.

7. Da keiner der Einwände der Beschwerdeführerin eine Lösung der objektiven Aufgabe gemäß dem Kennzeichen von

Anspruch 1 nahelegt, konnte die Beschwerdeführerin nicht schlüssig belegen, dass es dem Gegenstand von Anspruch 1 an der erfinderischen Tätigkeit fehlt.

Entscheidungsformel

Aus diesen Gründen wird entschieden:

Die Beschwerde wird zurückgewiesen.

Die Geschäftsstellenbeamtin Die Vorsitzende

K. Götz A. Ritzka